

2023-10-17

TJÄNSTESKRIVELSE

Dnr: UBN-2023-00157

Revisionskrivelse och revisionsrapport 4 2023 – Granskning av kommunens hantering av skyddade personuppgifter

Yttrande till kommunfullmäktiges revisorer

Förslag till beslut

Utbildningsnämnden antar yttrande över revisionsrapport och revisionskrivelse enligt bilaga 3 till tjänsteskrivelse daterad 2023-10-17.

Sammanfattning av ärendet

EY har på uppdrag av Nacka kommuns revisorer granskat kommunens hantering av skyddade personuppgifter. Syftet med granskningen har varit att bedöma hur kommunen säkerställer att skyddade personuppgifter inte röjs till obehöriga samt om kommunens rutiner är ändamålsenliga och tillämpade. Detta har avsett skyddade personuppgifter för både medborgare och anställda vid kommunen. Granskningen har omfattat kommunstyrelsen, socialnämnden, utbildningsnämnden samt nämnden för arbete och försörjning.

Utifrån revisorernas rekommendationer har ett yttrande för utbildningsnämnden tagits fram utifrån de rekommendationer som revisorerna lämnat gällande utbildningsnämnden.

Ärendet

Innehållet i revisionsgranskningen i korthet samt revisorernas rekommendationer
EY har på uppdrag av Nacka kommuns revisorer granskat kommunens hantering av skyddade personuppgifter. Syftet med granskningen har varit att bedöma hur kommunen säkerställer att skyddade personuppgifter inte röjs till obehöriga samt om kommunens rutiner är ändamålsenliga och tillämpade. Detta har avsett skyddade personuppgifter för både medborgare och anställda vid kommunen. Granskningen har omfattat kommunstyrelsen, socialnämnden, utbildningsnämnden samt nämnden för arbete och försörjning.

Revisorernas övergripande bedömning är att kommunstyrelsen och de granskade nämnderna inte har säkerställt att skyddade personuppgifter inte röjs till obehöriga. De olika enheterna har vidtagit diverse åtgärder i sitt löpande arbete för att förhindra röjning av skyddade personuppgifter, men revisorernas bedömning är att även om Nacka kommuns styrmodell är politiskt beslutad är en strategisk inriktning inom området nödvändig. Det genomförs ingen systematisk och kommunövergripande fortlöpande kompetensutveckling inom området och det finns inget särskilt utrymme för rutinförankring. Enheterna genomför själva en viss rutinförankring och kompetensutveckling genom att löpande behandla frågan internt på möten. Revisorernas bedömning är dock att det finns ett behov av att utbilda samtliga medarbetare i hanteringen av skyddade personuppgifter specifikt och att det bör ske regelbundet i syfte att hålla kunskapen vid liv över tid.

Kommunstyrelsen och samtliga granskade nämnder rekommenderas att:

- Upprätta risk- och konsekvensanalyser avseende hanteringen av skyddade personuppgifter. Vid behov inkludera området i internkontrollplanerna.
- Upprätta och anta styrande dokument för hanteringen av skyddade personuppgifter inom det egna ansvarsområdet. Dessa bör vara av övergripande karaktär.
- Genomföra obligatoriska utbildningar för samtlig personal i tillämpning av styrande dokument samt hanteringen av skyddade personuppgifter regelbundet. Säkerställ samtidigt att enheternas arbetsrutiner för hantering av skyddade personuppgifter är förankrade hos medarbetarna, exempelvis som en del av årshjul.
- Begränsa åtkomsten till personuppgifterna genom strikt behörighetstilldelning.
- Genomföra kontroller av användarloggar som en organisatorisk säkerhetsåtgärd för att minska riskerna för röjning av skyddade personuppgifter.
- Säkerställa möjligheten att systematiskt följa upp avvikelser avseende skyddade personuppgifter.

Utbildningsnämnden och nämnden för arbete och försörjning rekommenderas att:

- Utvärdera riskerna för arbetet med skyddade personuppgifter med att arbets- och etableringsenheten och utbildningsenheten delar kontorslokal.

Utbildningsenhetens utredning samt förslag på yttrande

Denna tjänsteskrivelse avser enbart de rekommendationer som revisorerna lämnat till utbildningsnämnden. Av nedan följer utbildningsenhetens bedömning avseende de olika rekommendationer som revisorerna lämnar i ärendet.

Upprätta risk- och konsekvensanalyser avseende hanteringen av skyddade personuppgifter. Vid behov inkludera området i internkontrollplanerna.

Utbildningsenheten har för avsikt att som en del i enhetens eget kvalitetsarbete genomföra risk- och konsekvensanalyser årligen med medarbetare som har arbetsuppgifter där de hanterar skyddade personuppgifter.

Utbildningsnämndens internkontrollplan bygger på en genomförd väsentlighets- och riskanalys. Om nämnden identifierar att hanteringen av skyddade personuppgifter har ett högt riskvärde blir risken ett område som förs in i nämndens internkontrollplan, men så har hittills inte varit fallet.

Upprätta och anta styrande dokument för hanteringen av skyddade personuppgifter inom det egna ansvarsområdet. Dessa bör vara av övergripande karaktär.

Att anta ett styrande dokument inom utbildningsnämndens ansvarsområde bedöms i dagsläget inte vara nödvändigt. Det viktigaste är i stället att interna rutiner regelbundet ses över och revideras och är kända av samtliga medarbetare så att skyddade personuppgifter hanteras korrekt.

Genomföra obligatoriska utbildningar för samtlig personal i tillämpning av styrande dokument samt hanteringen av skyddade personuppgifter regelbundet. Säkerställ samtidigt att enheternas arbetsrutiner för hantering av skyddade personuppgifter är förankrade hos medarbetarna, exempelvis som en del av årshjul.

Frågan om hantering av skyddade personuppgifter läggs nu in i planeringen årshjulet för vad som tas upp på APT för samtliga medarbetare.

Medarbetare som ofta hanterar personuppgifter ges redan möjlighet att delta i särskild kompetensutveckling. Utbildningsenheten kommer att ta del i det arbete som pågår i kommunen när det gäller lämpliga utbildningsinsatser för medarbetare vid nyanställning och återkommande utbildningsinsatser.

Begränsa åtkomsten till personuppgifterna genom strikt behörighetstilldelning.

Uppgifter för personer med skyddade personuppgifter hanteras i en särskild del i verksamhetssystemet för förskola och grundskola där enbart det fåtal medarbetare som arbetar med dessa uppgifter har behörighet. Hanteringen av uppgifter för personer med

skyddade personuppgifter säkerställs också i den upphandling som nu genomförs av nytt verksamhetssystem för förskola och skola.

Genomföra kontroller av användarloggar som en organisatorisk säkerhetsåtgärd för att minska riskerna för röjning av skyddade personuppgifter.

Loggkontroller genomförs vid behov, exempelvis när man upptäcker att ett ärende har hanterats felaktigt. Behovet av systematiska kontroller av användarloggar framöver kommer att ses över i samband med risk- och konsekvensanalys av hanteringen av skyddade personuppgifter.

Säkerställa möjligheten att systematiskt följa upp avvikelser avseende skyddade personuppgifter.

Avvikelse vad gäller skyddade personuppgifter innebär som huvudregel att en så kallad personuppgiftsincident även inträffar. Då skyddade personuppgifter anses vara en ”extra skyddsvärd personuppgift” enligt dataskyddsförordningen innebär det att avvikelser/incidenter kopplat till denna form av personuppgift ska anmälas som en personuppgiftsincident till kommunens dataskyddssombud. Vid allvarigare överträdelser ska en anmälan även ske till Integritetsskyddsmyndigheten, IMY.

Personuppgiftsincidenter följs årligen upp av kommunens dataskyddssombud i respektive nämnd i samband med dataskyddssombudets årsrapport. Beslut avseende personuppgiftsincidenter på utbildningsnämndens ansvarsområde fattas på delegation av utbildningsenhetens enhetschef och anmäls till nästkommande nämndsammanträde. Genom att delegationsbeslut anmäls på nämndsammanträdena får både nämnden och allmänheten en insyn i anmälda incidenter. Det kan således konstateras att det finns upparbetade rutiner för avvikelshantering inom området.

Utvärdera riskerna för arbetet med skyddade personuppgifter med att arbets- och etableringsenheten och utbildningsenheten delar kontorslokal

Beaktandet av sekretess gäller all hantering av personuppgifter, oavsett om det avser en person som har skyddade personuppgifter eller inte. Utbildningsenheten har inte identifierat negativa påverkansfaktorer som specifikt kan drabba personer med skyddade personuppgifter kopplat till att arbets- och etableringsenheten och utbildningsenheten delar kontorslokaler. Samtliga anställda på båda enheterna är väl förtrogna med offentlighet- och sekretesslagstiftningen.

Nacka kommuns övergripande arbetssätt i Nacka stadshus är baserat på öppna kontorslandskap sedan flera år tillbaka. Alla enheter utgår från en så kallad hemvist. Arbetsmodellen innebär att det är så kallad fri sittning i stadshuset samt att alla

medarbetare kan boka merparten av de mötes- och konferensrum som finns att tillgå, även i andra kontorslandskap än den egna hemvisten. Arbetsättet medför att det är många personer i rörelse i stadshuset. Att arbeta i öppna kontorslandskap ställer krav på den enskilde medarbetarens ansvar, särskilt i frågor avseende sekretess.

I enlighet med det systematiska arbetsmiljöarbetet genomförs risk- och konsekvensbedömningar vid organisatoriska förändringar i verksamheten, och detta genomfördes i samband med flytten till den gemensamma hemvisten. Vid dessa risk- och konsekvensbedömningar har frågan om risken för att personuppgifter och sekretessbelagd information röjs med anledning samlokaliseringen identifierats. Risken har undersökts, riskbedömts och beslutade åtgärder har vidtagits vilka följs upp i enlighet med det systematiska kvalitetsarbetet.

Ett gemensamt enhetsmöte mellan arbets- och etableringsenheten och utbildningsenheten genomfördes i samband med samlokaliseringen med fokus på dialog specifikt kring sekretessfrågan. Arbets- och etableringsenheten och utbildningsenheten har en väl utvecklad samverkan och regelbunden översyn med uppföljning av kontorslandskapets spelregler. Syftet med samverkan är att identifiera utvecklings- och förbättringsåtgärder men också påtala vad som fungerar bra och vad som har förbättrats sedan sist.

Ekonomiska konsekvenser

Förslaget till beslut om yttrande medför inga ekonomiska konsekvenser.

Konsekvenser för barn

Förslaget till beslut om yttrande innebär att hanteringen av skyddade personuppgifter för barn säkras ytterligare. En god hantering är mycket väsentlig och ges hög prioritet av utbildningsenheten.

Handlingar i ärendet

Tjänsteskrivelse daterad den 17 oktober 2023

Bilaga

1. Revisionskrivelse 2023-05-24
2. Revisionsrapport 4, 2023
3. Förslag på yttrande

Carina Legerius
Enhetschef
Utbildningsenheten

Annica Bergström
Biträdande enhetschef
Utbildningsenheten

